APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,099	04/09/2001	Binyamin Pinkas	704-X00-47US	2969

27317	7590	11/02/2005		

FLEIT KAIN GIBBONS GUTMAN BONGINI & BIANCO
21355 EAST DIXIE HIGHWAY
SUITE 115
MIAMI, FL 33180

. EXAMINER
SON, LINH L D

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>09 April 2001</u>.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-22</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-22</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   This Office Action is responding to the Amendment received on 8/18/05 received

on. This is a Non-Final Action.

2.   Claims 1-22 are pending.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4.   Claims 1-3, 5-9, 11, and 16-22 are rejected under 35 U.S.C. 102(e) as being

anticipated by Ausubel, US/5905975.

5.   As per claims 1 and 2:

Ausubel discloses "A method for preserving the integrity of a negotiation

comprising the steps of: a) providing an architecture which includes a center A (Fig 1),

and a plurality of users B_1, B_2 to B_n (Fig 1, Col 24 lines 40-50, and Col 26

lines 5-20), b) generating for each user B_i an input X_i (Col 26 lines 20-40), c)

inputting each user's input X.sub.i to the center A (Col 26 lines 20-40), d) computing and

publishing a function F (X.sub.1, X.sub.2 to X.sub.n) (subroutine) by the center A based

on the input messages it receives (Col 26 line 65 to Col 27 line 12), e) each user B.sub.i

(1<= i<= n) communicating with the center A exclusively (Col 21 lines 10-35), and

publishing by center A to each of the users additional information which let each of the

users verify that F was computed correctly, and preventing a coalition of any one subset

of the users from learning (i) anything which cannot be computed just from the output of

the function, F(X.sub.1 to X.sub.n), and from their own inputs, and (ii) information about

the inputs of other users (Col 25 lines 59 to Col 26 line 4, and Col 27 lines 1-13).

6.   As per claim 3:

Ausubel discloses "the method according to any one of claims 1, for computing

the output of a sealed bid auction (Col 21 lines 10-35), where the users are bidders and

the center is the auctioneer, and wherein the input X.sub.i is the bid of bidder B.sub.i,

and an output of F is the identity of the winning bidder and the amount to be paid, and

wherein the center only makes disclosure to the winning bidder, while all other bidders

being able to verify that the auction was computed correctly, but do not learn any other

information (Col 25 lines 59 to Col 26 line 4).

7.   As per claim 5:

Ausubel discloses "discloses the method according claims 1, for second price auctions

(Vickrey auctions), where the output of F is (B.sub.j1, X.sub.j2), where X.sub.j1 is

greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is greater or equal to any X.sub.i for 1 <=i <=n except for i=j1" in (Col 25 lines 1-20).

8.   As per claim 6:

Ausubel discloses "the method according to claims 1, for k-th price auctions, where the output of F is (B.sub.j1, X.sub.j2), where X.subj1 is greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is the k-th largest among all inputs X.sub.i for 1<=i<=n" in (Col 25 lines 1-45).

9.   As per claim 7:

Ausubel discloses "the method according to claim 1 wherein the auction is a plural auction where there is a plurality of sellers" in (Col 7 lines 25-35)

10.   As per claim 8:

Ausubel discloses "discloses the method according to claim 1 wherein the auction is a generalized Vickrey auction" in (Col 4 lines 55-67)

11.   As per claim 11:

Ausubel discloses "discloses the method according to claim 1, comprising the step of computing the output of the function such that only the center learns the output of the function or several of the users learn the output of the function, or all the users learn the output of the function" in (Col 25 lines 59 to Col 26 line 4).

12.   As per claim 16:

Ausubel discloses "discloses the method according to claim 1, comprising the step of computing a function by N centers, such that only if K of the N centers collude they can learn information about the parties inputs

13.   As per claims 17-18, and 22:

Ausubel discloses "Secure Auction Systems" invention, which includes a system that contains N parties (Fig 1), each having a private input" (Col 21 lines 10-35), and "a center adapted to compute a function F of said input apparatus for computing said function F in said center, comprising: a first program (subroutine) provided in the center that enables calculation of said function F" in (Col 26 lines 20-65); circuitry for publishing said function F using the program while not revealing substantially any information about said input (Col 8 lines 1-17, and Col 26 line 65 to Col 27 line 12); "a second program provided to the parties enabling each one of said parties to prove that said function F was calculated correctly" in (Col 27 lines 4-11, the calculation of the result of everybody else with the bid of user I to get the proof, which will equal to the information in the message sent).

14.   As per claim 19:

Ausubel discloses "a system according to claim 17, wherein the second program precludes the learning of any information other than the function F was calculated correctly in a system according to claim 17, wherein the first program includes a construction of K garbled circuits for computing function F (Col 26 lines 20-65).

15.   As per claim 20:

Ausubel discloses "a system according to claim 17, wherein said parties are

bidders in an auction, said input are bids, said center is an auctioneer, said function F is

the rule by which said auction is decided, whereby the auctioneer is capable of

calculating the result of said auction without revealing any information about said bids,

except for the identity of the winning party from among said parties, and the amount to

pay (Col 26 line 65 to Col 27 line 12).

16.   As per claim 21:

Ausubel discloses "a system according to claim 20, wherein Ausubel inherently

teach the function is determined utilizing a circuit of gates" in (Col 8 lines 1-17).

Claim Rejections - 35 USC § 103

17.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

18.   Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ausubel

19.   As per claim 9:

Ausubel discloses the method according to claim 1. However, Ausubel does not

teach the step of, computing the auction such that the auctioneer wants to buy an item

and each of the bidders wants to sell this item, and wherein negative values of the

inputs X.sub.i are possible. Nevertheless, Ausubel does teach many types of auction

and method to carry out (Col 1 lines 38-67). Therefore, it is obvious at the time of the

invention was made for one having ordinary skill in the art that changing roles in an

auction is explicitly teach and would have been obvious for one having ordinary skill in

the art to implement.

20.   Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ausubel

         in view of Shoham (US 6285989) (cited in 892 dated 05/19/05).

21.   As per claim 10:

         Ausubel discloses "the method according to claim 1". However, Ausubel does

not teach "comprising the step of; computing the output of the auction such that the

users learn, in addition, some statistic of the inputs, such as, the users can learn at least

one of the average of the inputs, the variance of the inputs, or how many one inputs

were in a certain range"

Nevertheless, Shoham does teaches "comprising the step of; computing the output of

the auction such that the users learn, in addition, some statistic of the inputs, such as,

the users can learn at least one of the average of the inputs, the variance of the inputs,

or how many one inputs were in a certain range" in (Col 15 lines 9-20).

Therefore, it would have been obvious at the time of the invention was made for one

having ordinary skill in the art to modify Ausubel's invention to include the average of

the inputs information in the message to provide information to the bidders.

22.   Claims 4, 8, and 12-14 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Ausubel in view of Ausubel (US 6021398), hereinafter '398.

(cited in 892 dated 05/19/05)

23.   As per claim 4:

Ausubel discloses the method according to claims 1 and the first price auctions

(Col 1 lines 38-42). However, Ausubel does not elaborate the first price auctions, where

the output of F is ($B.sub.j$, $X.sub.j$), where $X.sub.j$ is greater or equal to any one $X.sub.i$

for 1 <=i <=n. Nevertheless, '398 does elaborate the first price auctions completely (Col

14 lines 48-67). Therefore, it is obvious at the time of the invention was made for one

having ordinary skill in the art to incorporate the '398's teaching with Ausubel to ensure

a great bidding process.

24.   As per claim 8:

Ausubel discloses the method according to claim 1. However, Ausubel does not

elaborate clearly that the auction is a generalized Vickrey auction (Col 6 Table 1).

Nevertheless, '398 does teach the Vickery auction clearly on Col 14 lines 48 to 65.

Therefore, it is obvious at the time of the invention was made for one having ordinary

skill in the art to incorporate the '398's teaching with Ausubel to clarify the Vickrey

auction process and provide a legitimate bidding result.

25.   As per claim 12:

Ausubel discloses the method according to claim 1. However, Ausubel does not

teach the step of, computing the output of a mechanism, in particular, for one of Groves-

clark mechanisms, opinion polling and stable matching. Nevertheless '398 does teach

the method to compute the output of the bidding session (Col 14 line 20 to Col 15 line

7). Therefore, it is obvious at the time of the invention was made for one having

ordinary skill in the art to incorporate to provide a legitimate bidding result.

26.   As per claims 13 and 14:

Ausubel discloses the method according to claim 1. However, Ausubel does not

discloses the steps of each user committing to the values of his input in a manner that

the user cannot change it afterwards, but hiding the input value from the center, at a

specific stage, the users opening their commitments to their inputs and revealing their

values to the center, which then computes the value of F in a manner the each of the

users can verify that the values that were used as inputs for computing F were the

values that were committed to by the users. Nevertheless, '398 discloses the

"Computer Implemented Methods and Apparatus For Auctions" invention, which

teaches steps to secure the bidding value until the opening time (Col 20 lines 39-65).

Therefore, it is obvious at the time of the invention was made for one having ordinary

skill in the art to incorporate the '398's teaching with Ausubel to create a high integrity

bidding process.

27.   Claim **15** is rejected under 35 U.S.C. 103(a) as being unpatentable over Ausubel

(US 6285989) in view of Naor et al, hereinafter "Naor", (US 6055508). (cited in

892 dated 05/19/05)

28.   As per claim 15:

Ausubel discloses the method according to claim 1. Ausubel also teach the

Universal Surveillance Console (USC) which allow a third party to monitor the integrity

of the operation (Col 11 lines 1-20). However, Ausubel does not specifically teach the

step of computing a function where the center can generate a proof that it computed the

correct output of the function. Nevertheless, Naor discloses the "Method for Secure

Accounting and Auditing on a Communications Network" invention, which teaches a

method of providing an auditing party to certify multiple transactions between the

plurality clients and servers and able to correlate its calculation against the server

calculation to proof the result (Col 6 lines 11-60). Therefore, it is obvious at the time of

the invention was made for one having ordinary skill in the art to incorporate Naor's

method with Ausubel to add an additional integrity check in the bidding process.

Response to Arguments

29.   Applicant's arguments, see Amendment, filed on 08/18/05, with respect to the

rejection(s) of claim(s) 1-3, 5-8, 10-11, and 16 under 35 U.S.C. 102(e), claims 4,

9, and 12-15, 17-22 under 35 U.S.C. 103(a), have been fully considered and are

persuasive. Therefore, the rejection has been withdrawn. However, upon further

consideration, a new ground(s) of rejection is made in view of Ausubel, shoham, and Noar.

30.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

/Primary Examiner/
Art Unit 2135